

1/19

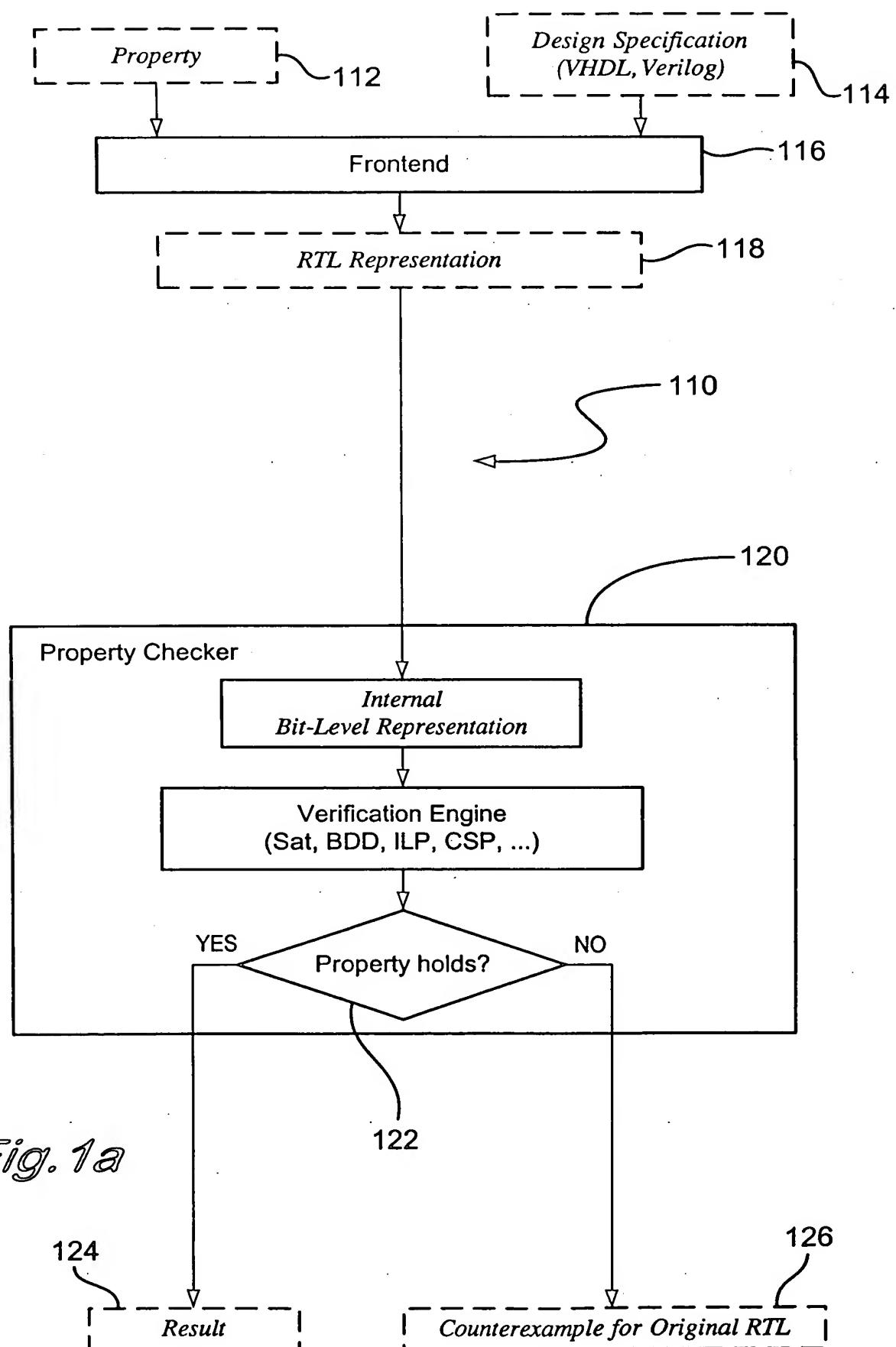
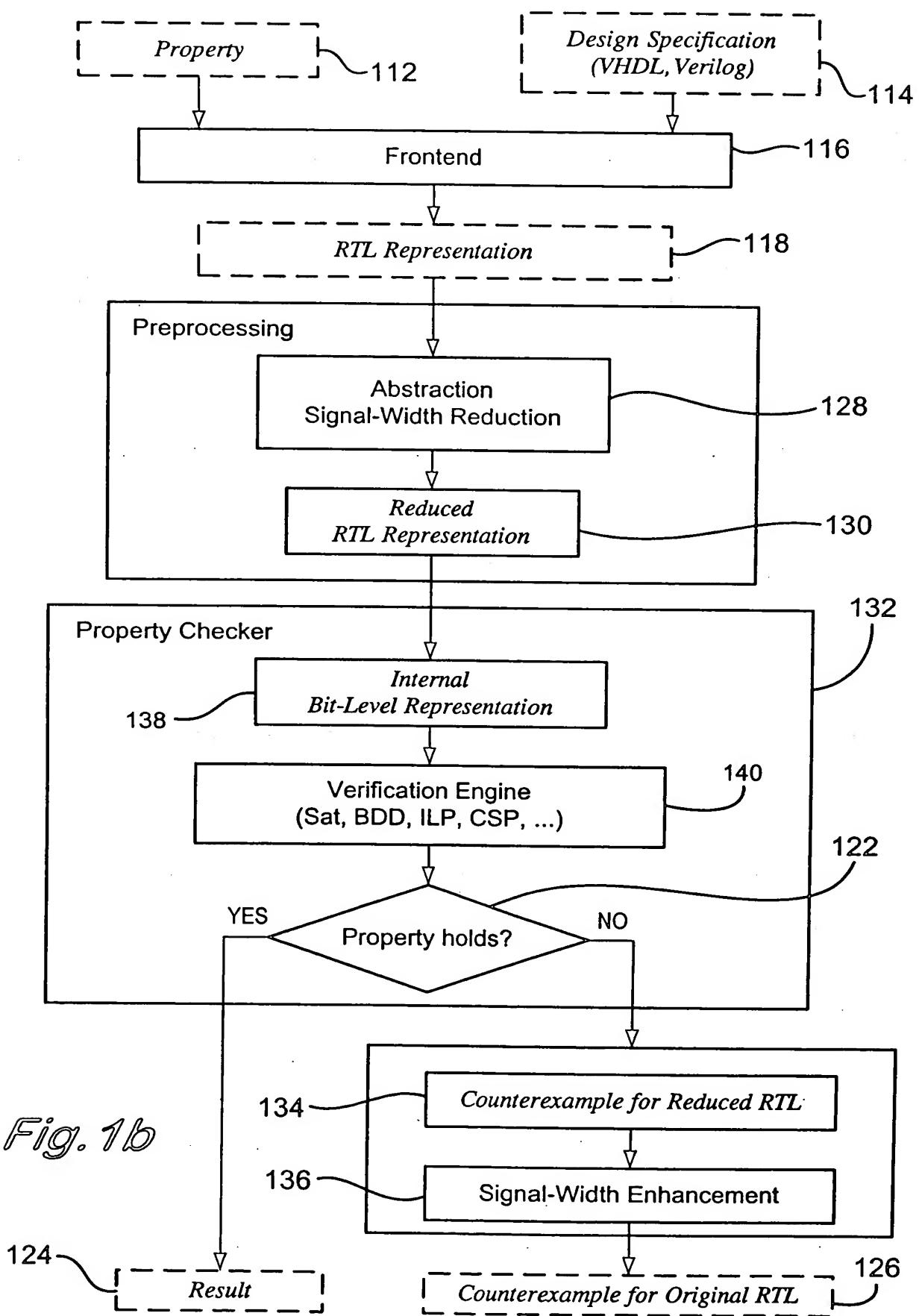
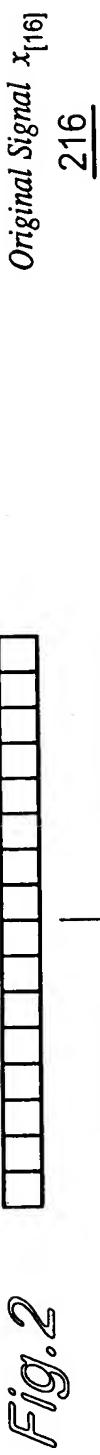


Fig. 1a

2/19



3/19

Fig. 2 

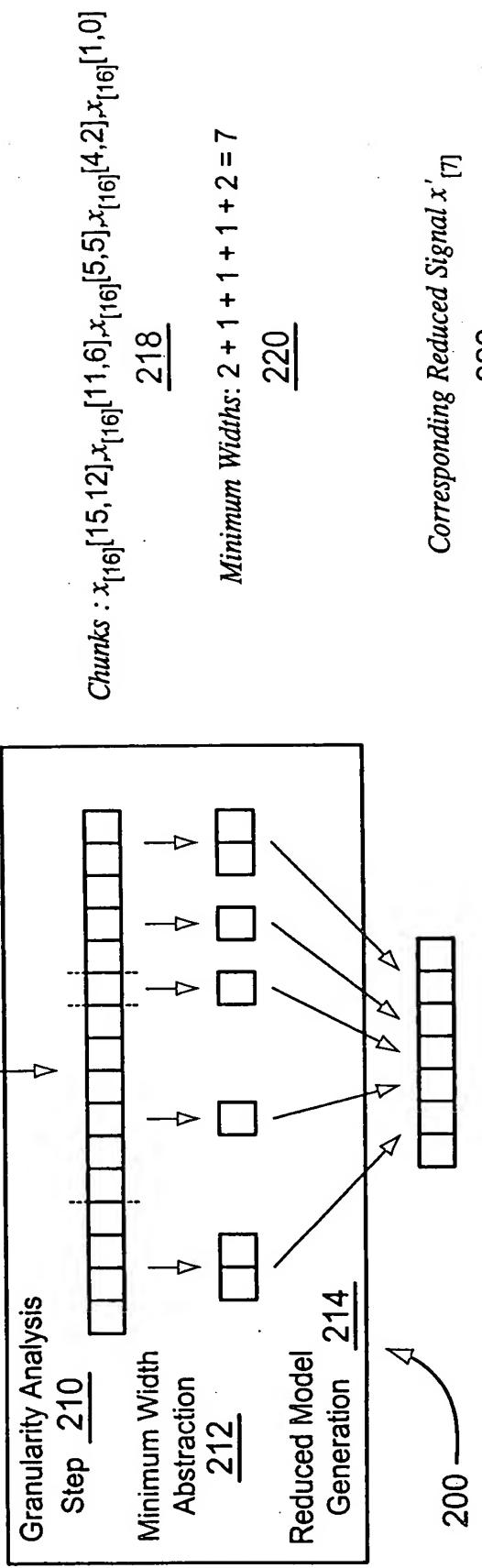
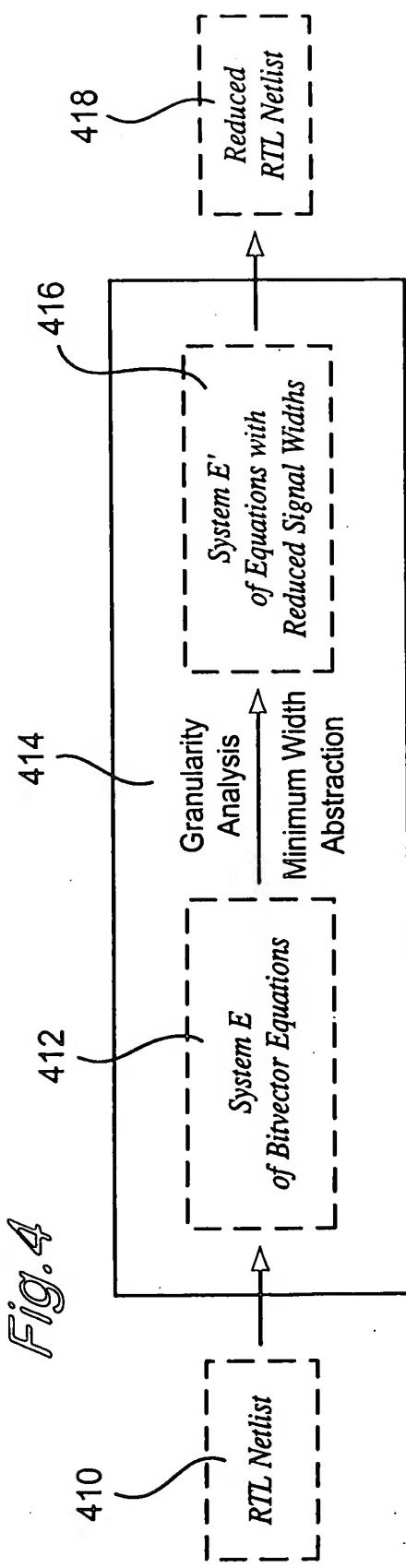


Fig. 4



4/19

Fig. 3

Bitvector Operator	Syntax	Example
bitvector variables bitvector constants	$x_{[n]}$ $c_{[m]}$	$x_{[8]}, y_{[1]}, z_{[4]}, \dots$ $10011_{[5]}, 0011111_{[8]}, 0_{[1]}, 1_{[1]}, \dots$
concatenation	\otimes	$x_{[16]} \otimes y_{[4]}$
extraction	$[j, i]$	$x_{[8]}[5, 2]$
bitwise negation (inversion)		$\text{neg}(x_{[8]})$
bitwise Boolean operations	and, or, xor nand, nor, xnor	$x_{[12]} \text{ and } y_{[12]}, x_{[12]} \text{ or } y_{[12]}, x_{[12]} \text{ xor } y_{[12]}$ $x_{[12]} \text{ nand } y_{[12]}, x_{[12]} \text{ nor } y_{[12]}, x_{[12]} \text{ xnor } y_{[12]}$
if-then-else	ite	$\text{ite}(a_{[4]} = b_{[4]}, x_{[8]}, y_{[8]})$ $\text{ite}(a_{[4]} < b_{[4]}, x_{[8]}, y_{[8]})$
arithmetic	$+, -, *$	$x_{[32]} + y_{[32]}, x_{[32]} - y_{[32]}$ $x_{[16]} * y_{[16]}$
memory read memory write	$\text{mem}_{[m..n]}[i_{[7]}]$	$x_{[10]} := \text{mem}_{[128..10]}[i_{[7]}]$ $\text{mem}_{[32..8]}[i_{[5]}] := x_{[8]}$

5/19

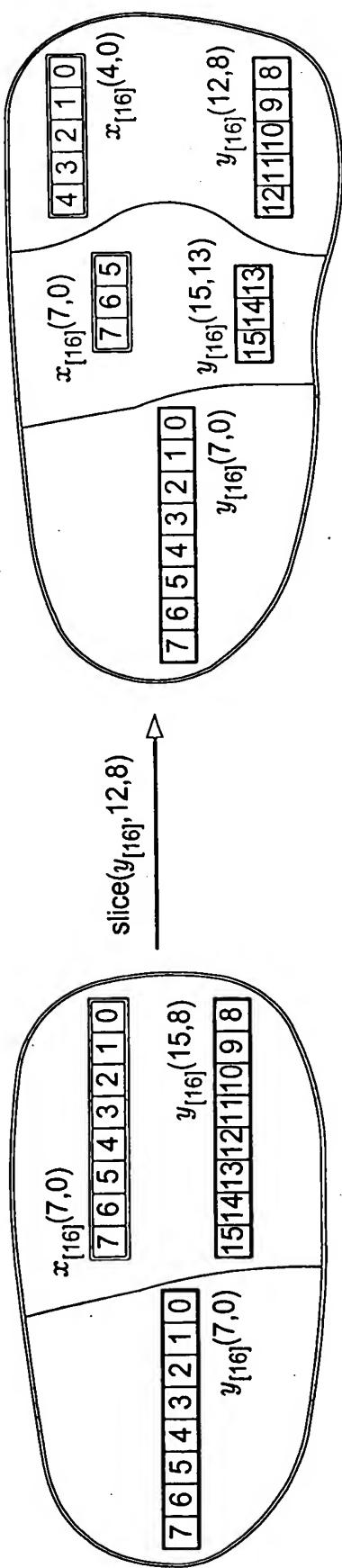


Fig. 5

Bitvectors

$$\begin{aligned}
 a_{[2]} &= \boxed{1 \ 0} \\
 x_{[8]} &= \boxed{7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1 \ 0} \\
 y_{[8]} &= \boxed{7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1 \ 0} \\
 z_{[4]} &= \boxed{3 \ 2 \ 1 \ 0}
 \end{aligned}$$

$x_{[8]} = y_{[8]}[7,4] \otimes x_{[8]}[3,2] \otimes a_{[2]}$
 $z_{[4]} = x_{[8]}[7,4]$ and $y_{[8]}[7,4]$

Dependency Classes of Bitvector Chunks

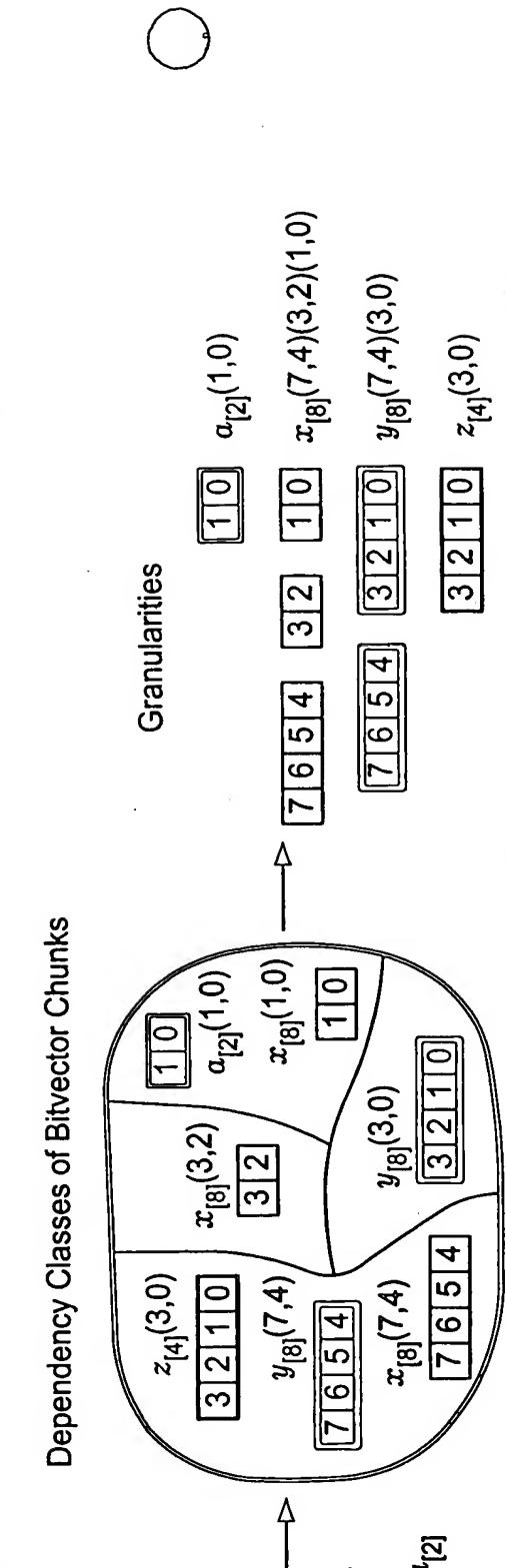


Fig. 6

Fig. 6a

Process 1 Granularity Analysis of Bitvector Equations

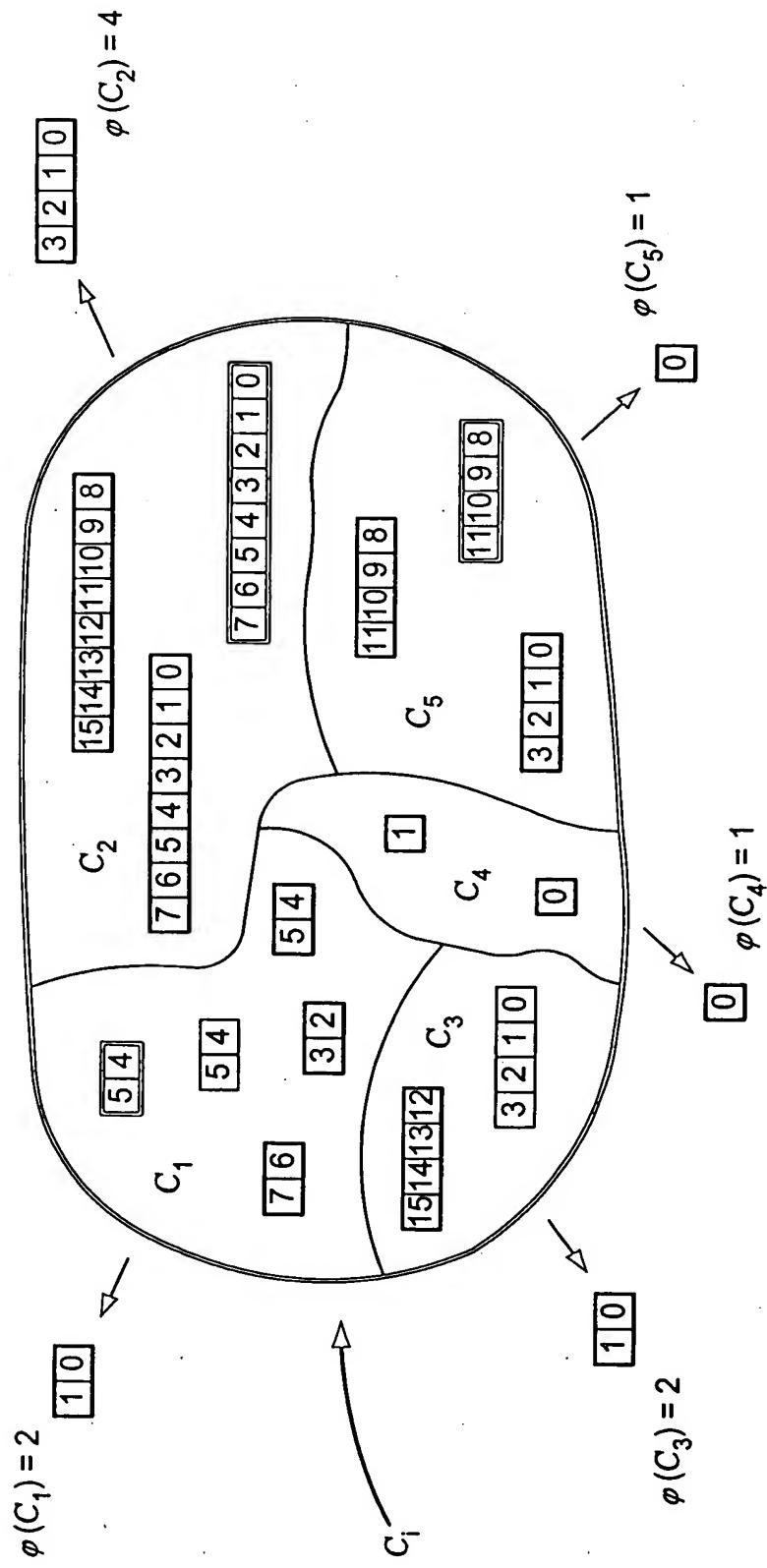
```

1 gran(e) {
2   switch (e) {
3     case e ≡ 's[n] = t1[m1] ⊗ t2[m2]' :
4       case e ≡ 's[n] = (t1[m1] ⊗ t2[m2])'[j, i]' :
5         gran('s[n][n-1, m2] = t1[m1]'); gran('s[n][m2-1, 0] = t2[m2]');
6           if (j < m2) {
7             gran('s[n] = t2[m2][j, i]');
8               } else if (i ≥ m2) {
9                 gran('s[n] = t1[m1][j-m2, i-m2]');
10                } else {
11                  gran('s[n] = t1[m1][j-m2, 0] ⊕ t2[m2][m2-1, i]');
12                }
13               gran('s[n] = t1[m1][k+j, k+i]');
14               gran('s[n] = b[m] = ite(a[m] = b[m], t1[m], te[n])[j, i]');
15               gran('s[n] = t1[m] and t2[m])[j, i]';
16               ...
17               case e ≡ 's[n] = neg(t[n])' :
18                 gran('s[n] = b[m]'); gran('s[n] = te[n]'); gran('s[n] = t2[n]');
19               case e ≡ 'x[n][j, i] = y[m][l, k]' :
20                 slice(x[n], j, i); slice(y[m], l, k); join(x[n][j, i], y[m][l, k]);
}

```

7/19

Fig. 7



8/19

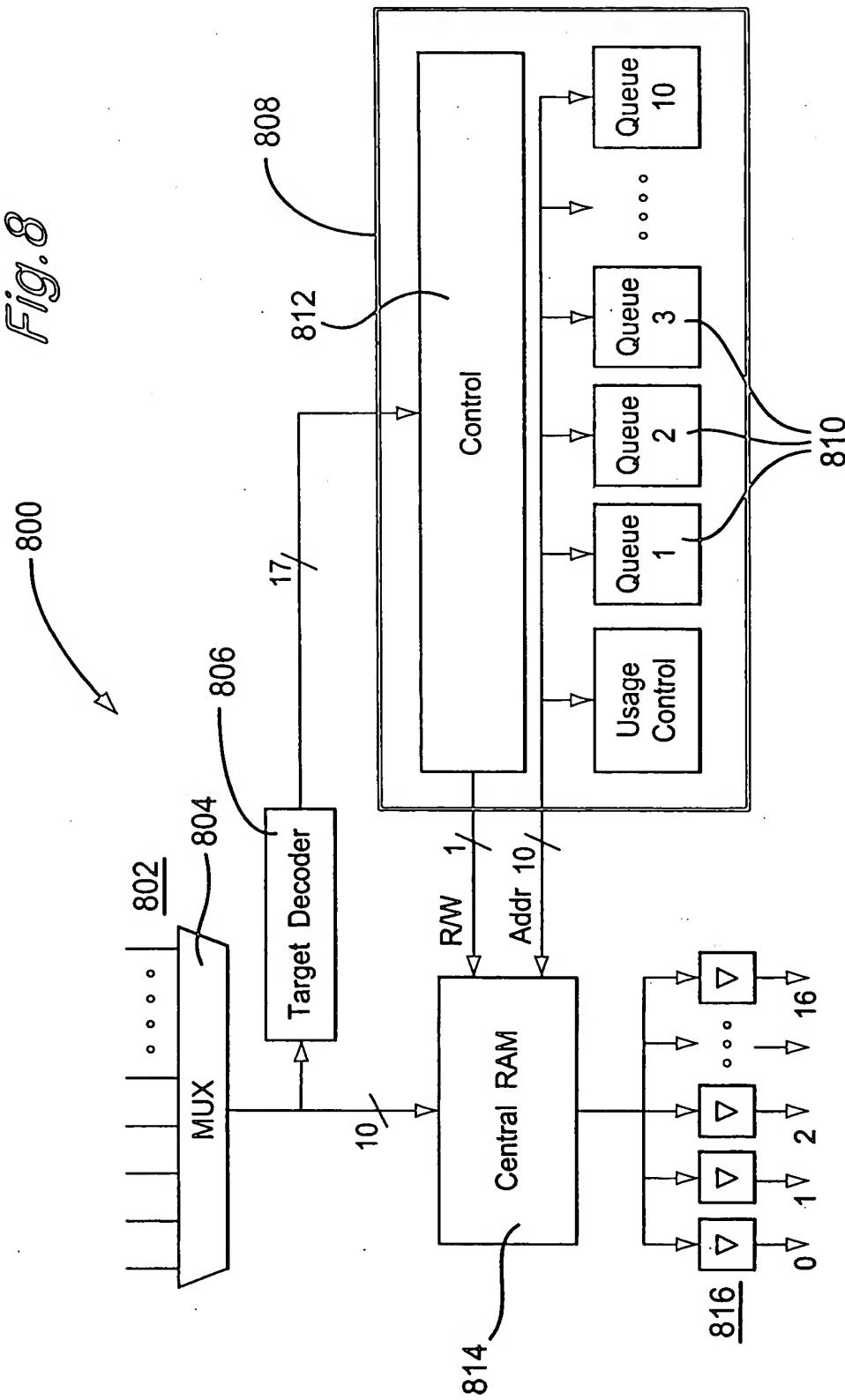
Fig. 7a

Process 2 Reduced Model Generation

```
1 for each bitvector variable  $x_{[n]}$  {
2    $m := 0$  ;
3   for each chunk  $x_{[n]} \langle j, i \rangle$  of the computed granularity of  $x_{[n]}$  {
4      $C := find(x_{[n]} \langle j, i \rangle)$  ; // equivalence class containing  $x_{[n]} \langle j, i \rangle$ 
5      $m := m + \varphi(C)$  ;
6   }
7   if ( $m \geq n$ ) then  $m := n$  ;
8   replace all occurrences of  $x_{[n]}$  in the bitvector equations by  $x'_{[m]}$  ;
9   and adjust all extraction expressions affected by  $x_{[n]}$  ;
10 }
```

9/19

Fig. 8

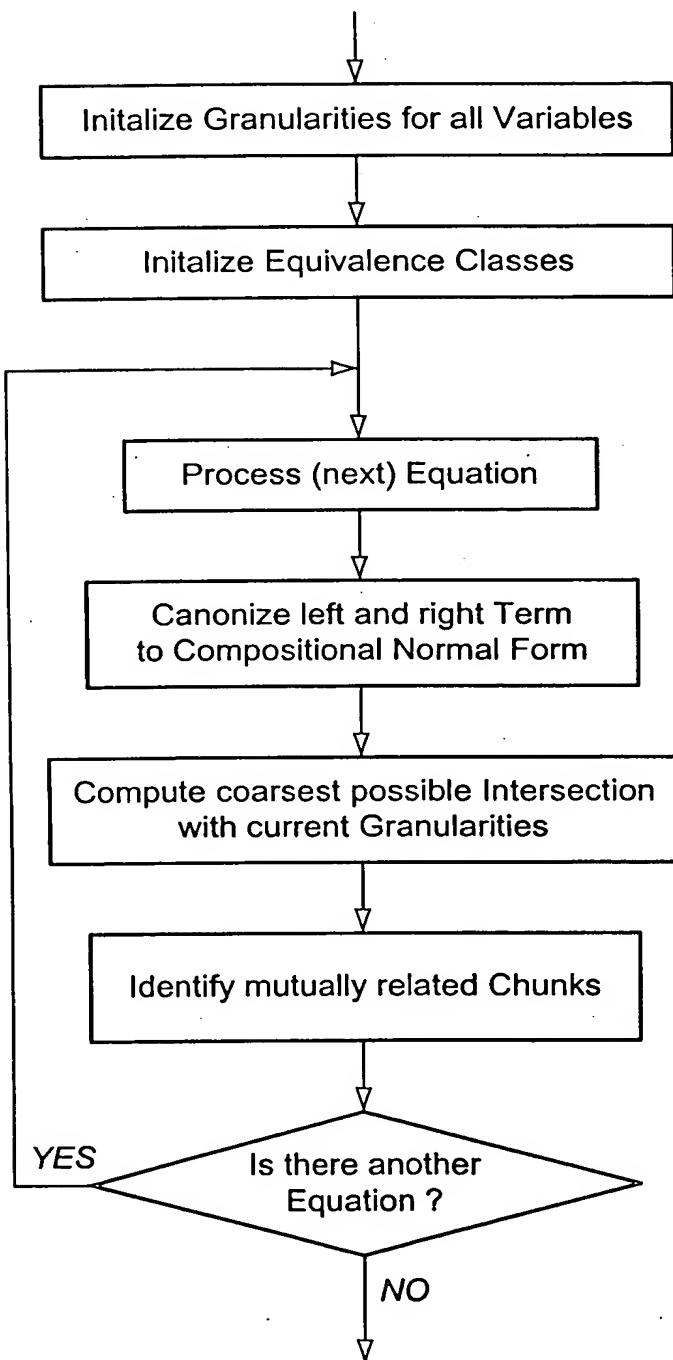


10/19

Fig. 9

	Property	Original design	Reduced model
Computation times of the prototype for analysis and reduced model generation	nop read write		2.96 secs 6.53 secs 3.24 secs
FIFO sizes on RTL	nop read write	160 cells x 10 bit 160 cells x 10 bit 160 cells x 10 bit	160 cells x 2 bit 160 cells x 3 bit 160 cells x 3 bit
Overall number of bits in all relevant signals (cones of influence of the property)	nop read write	20925 31452 14622	5034 (24.0 %) 10592 (33.6 %) 5163 (35.3%)
Overall number of gates in synthesized netlist	nop read write	23801 23801 23801	5661 (27.9 %) 7929 (33.3 %) 7929 (33.3 %)
Number of state bits	nop read write	1658 1658 1658	362 (21.8 %) 524 (31.6 %) 524 (31.6 %)
Property checker runtimes	nop read write_fail write_hold	23:33 min 42:23 min 2:08 min 27:08 min	37.96 secs (2.7 %) 3:27 min (8.1 %) 25.66 secs (19 .5 %) 1:08 min (4.2 %)

11/19



$$x_{[8]}[7,2] \otimes x_{[8]}[1,0] = \\ (a_{[4]} \otimes b_{[4]} \otimes c_{[4]})[11,4]$$

$$x_{[8]}[7,0] = a_{[4]}[3,0] \otimes b_{[4]}[3,0]$$

$$x_{[8]}[7,4] \otimes x_{[8]}[3,0] = \\ (a_{[4]}[3,0] \otimes b_{[4]}[3,0])$$

$$x_{[8]}[7,4] \longleftrightarrow a_{[4]}[3,0] \\ x_{[8]}[3,0] \longleftrightarrow b_{[4]}[3,0]$$

Fig. 10

12/19

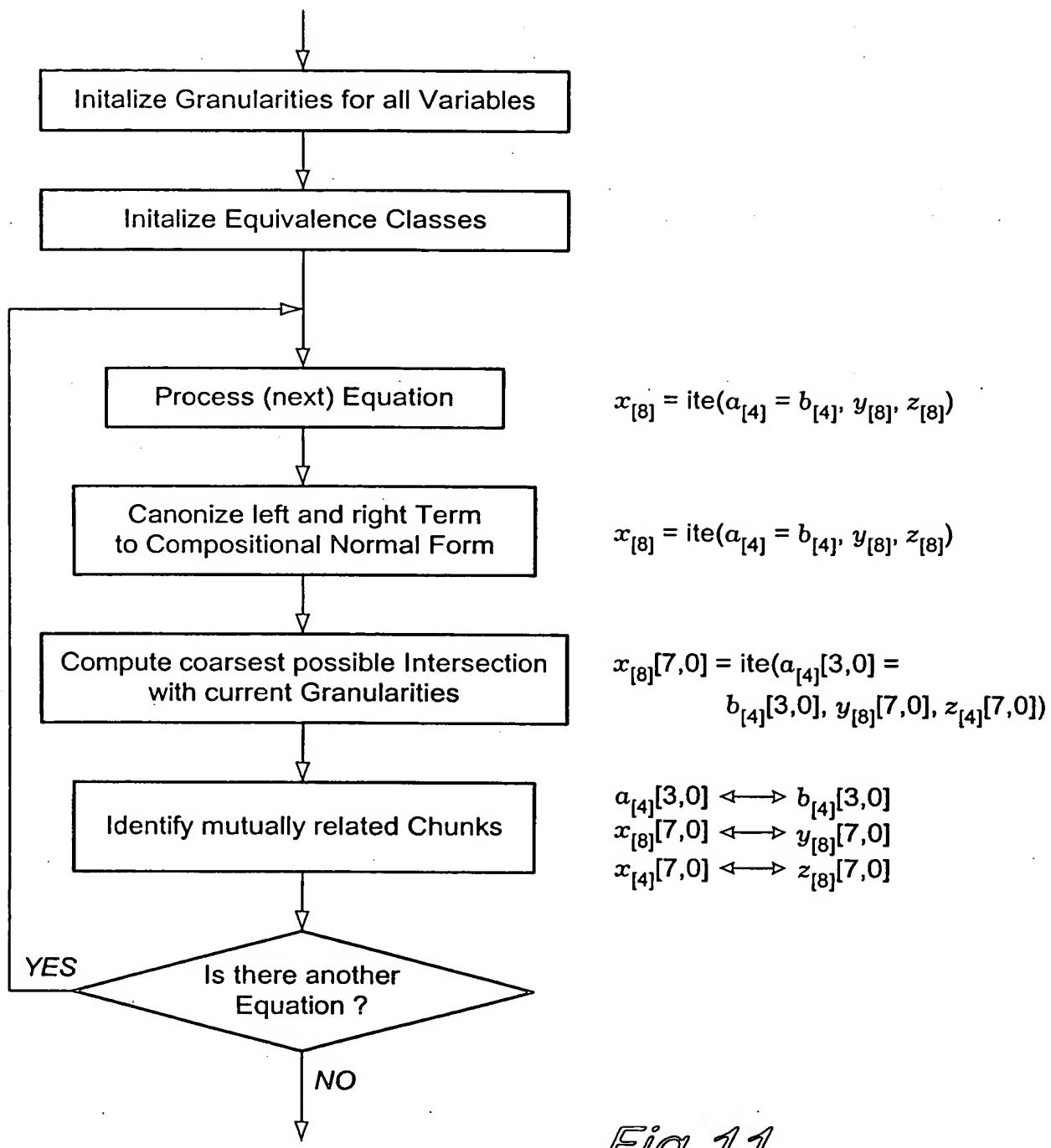


Fig. 11

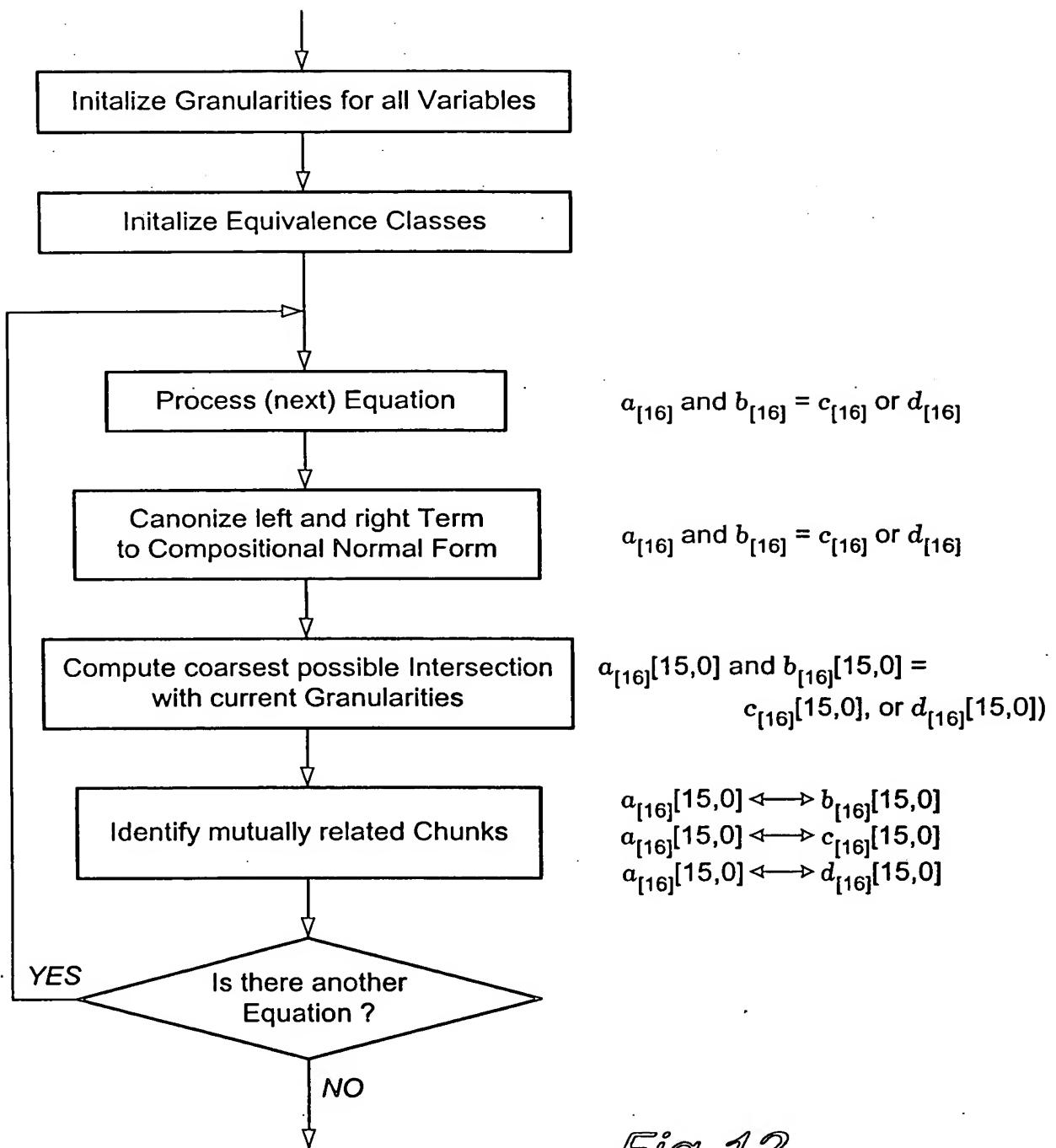
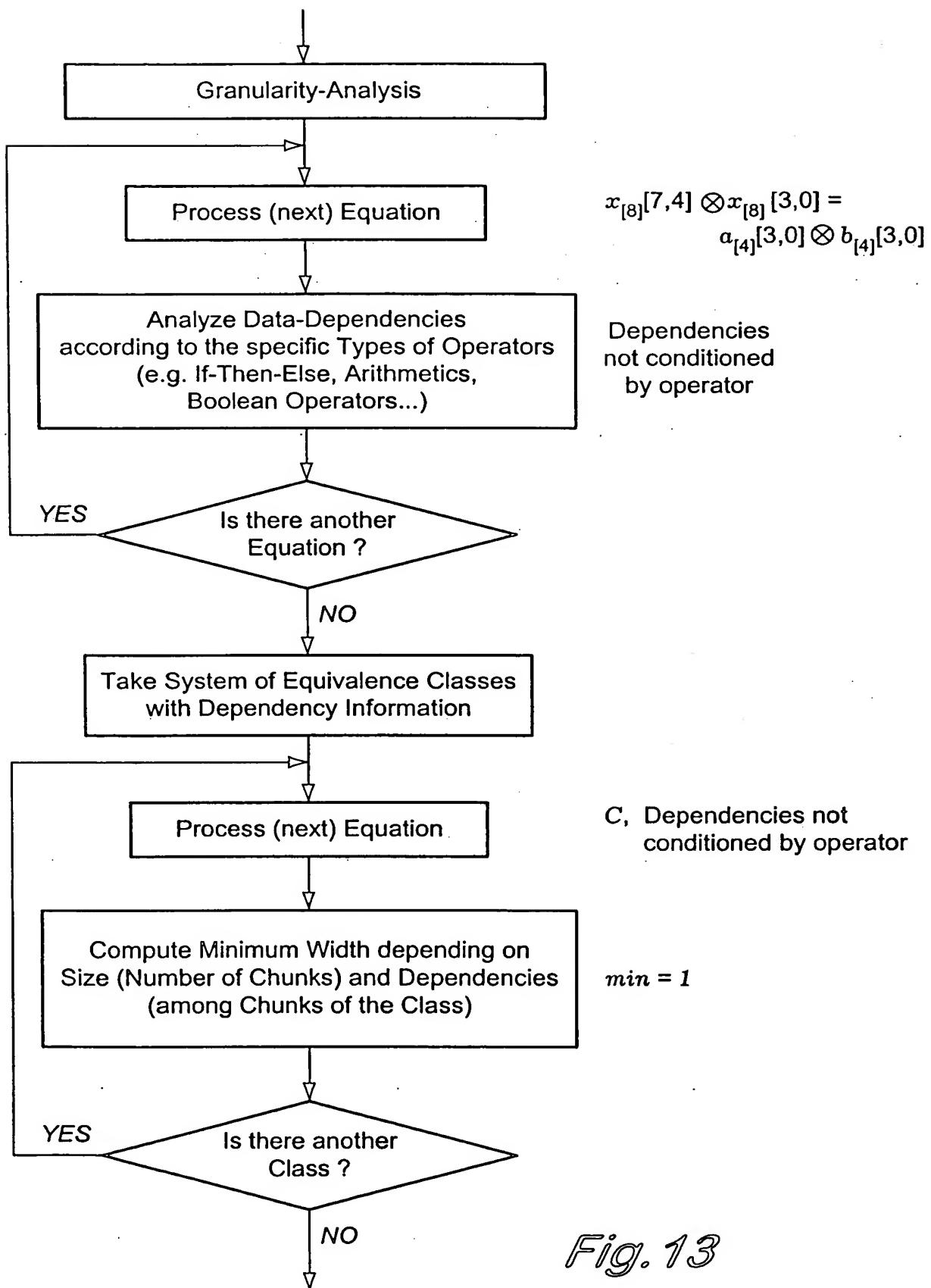
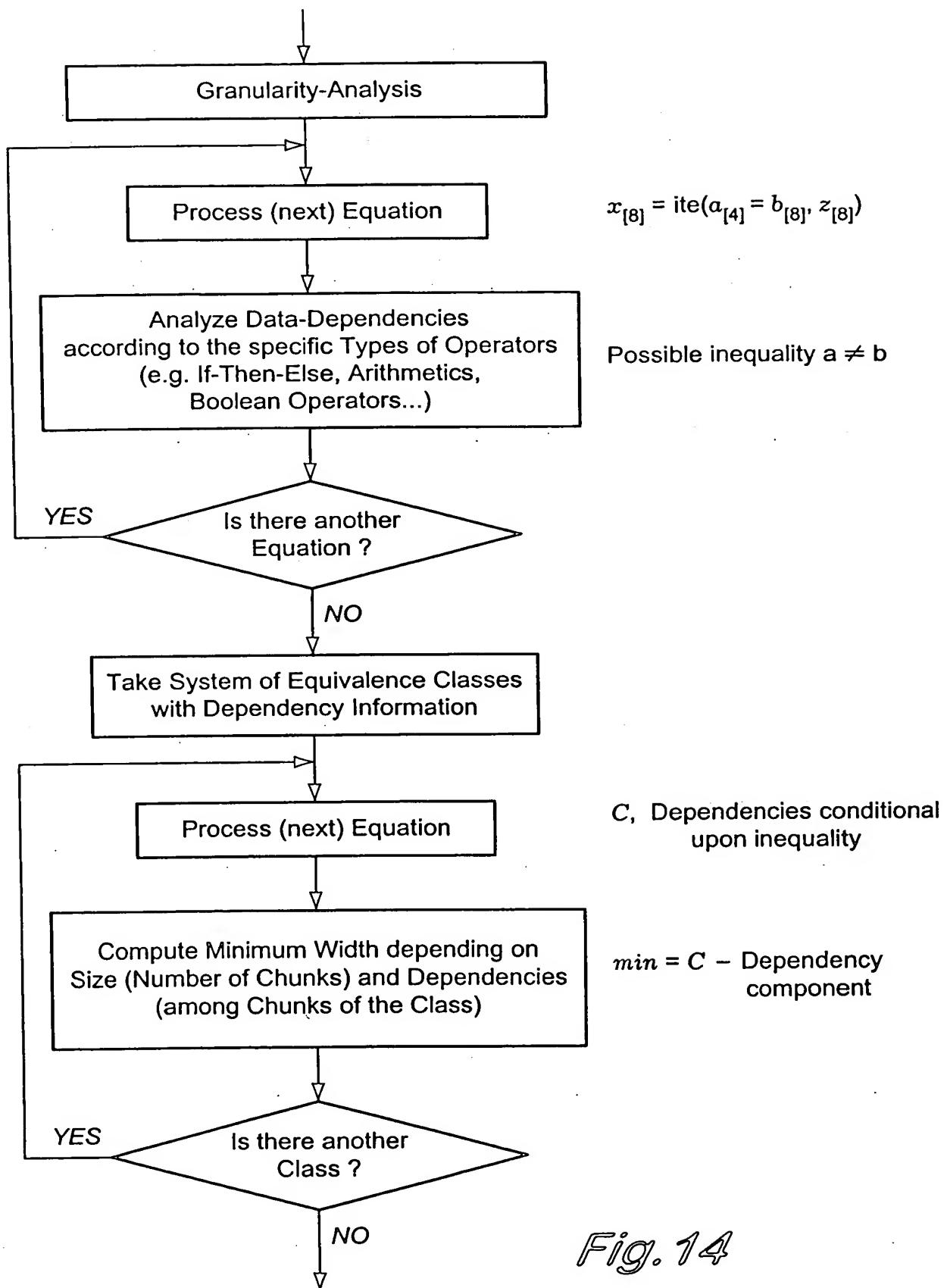


Fig. 12

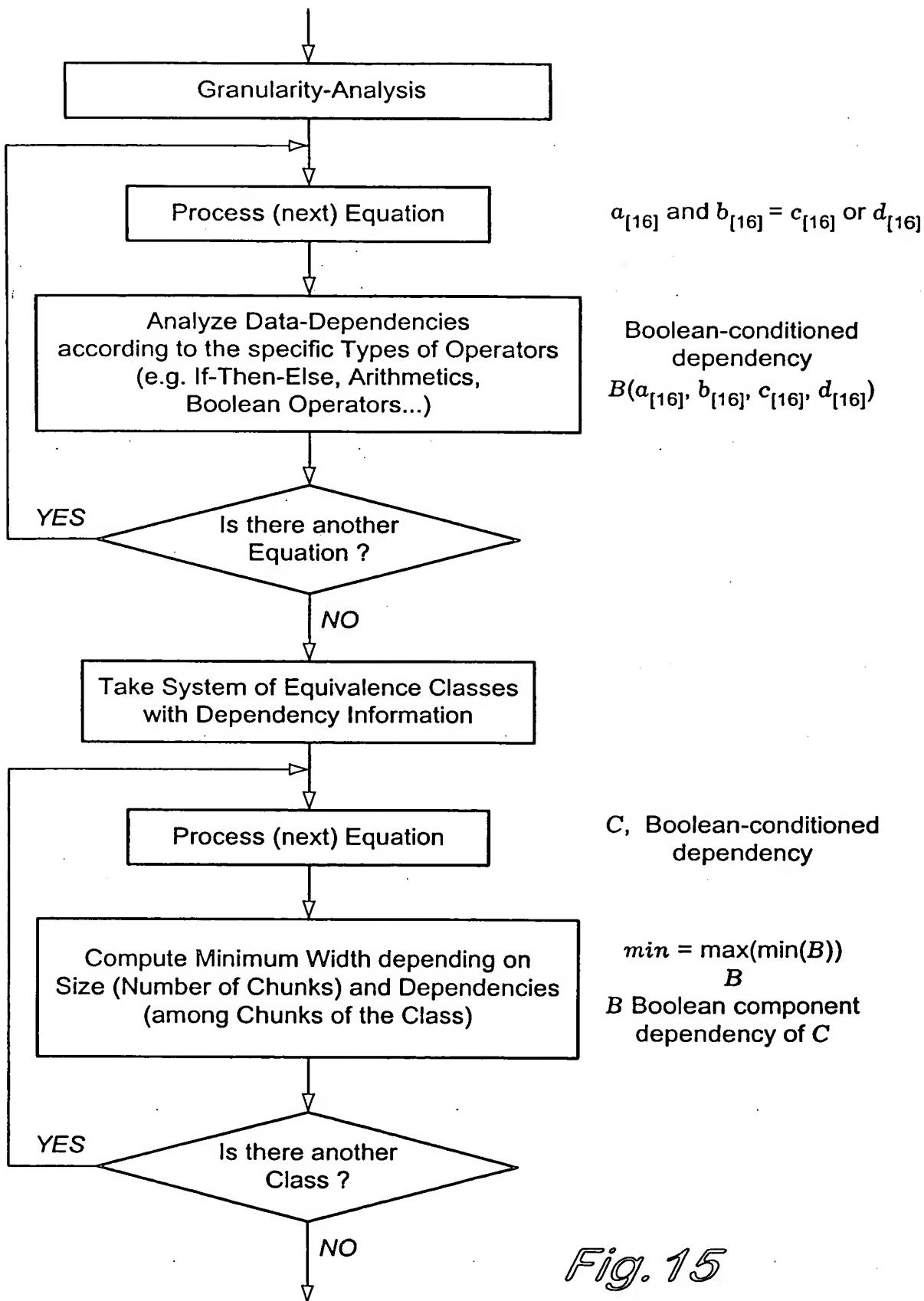
14/19



15/19



16/19



17/19

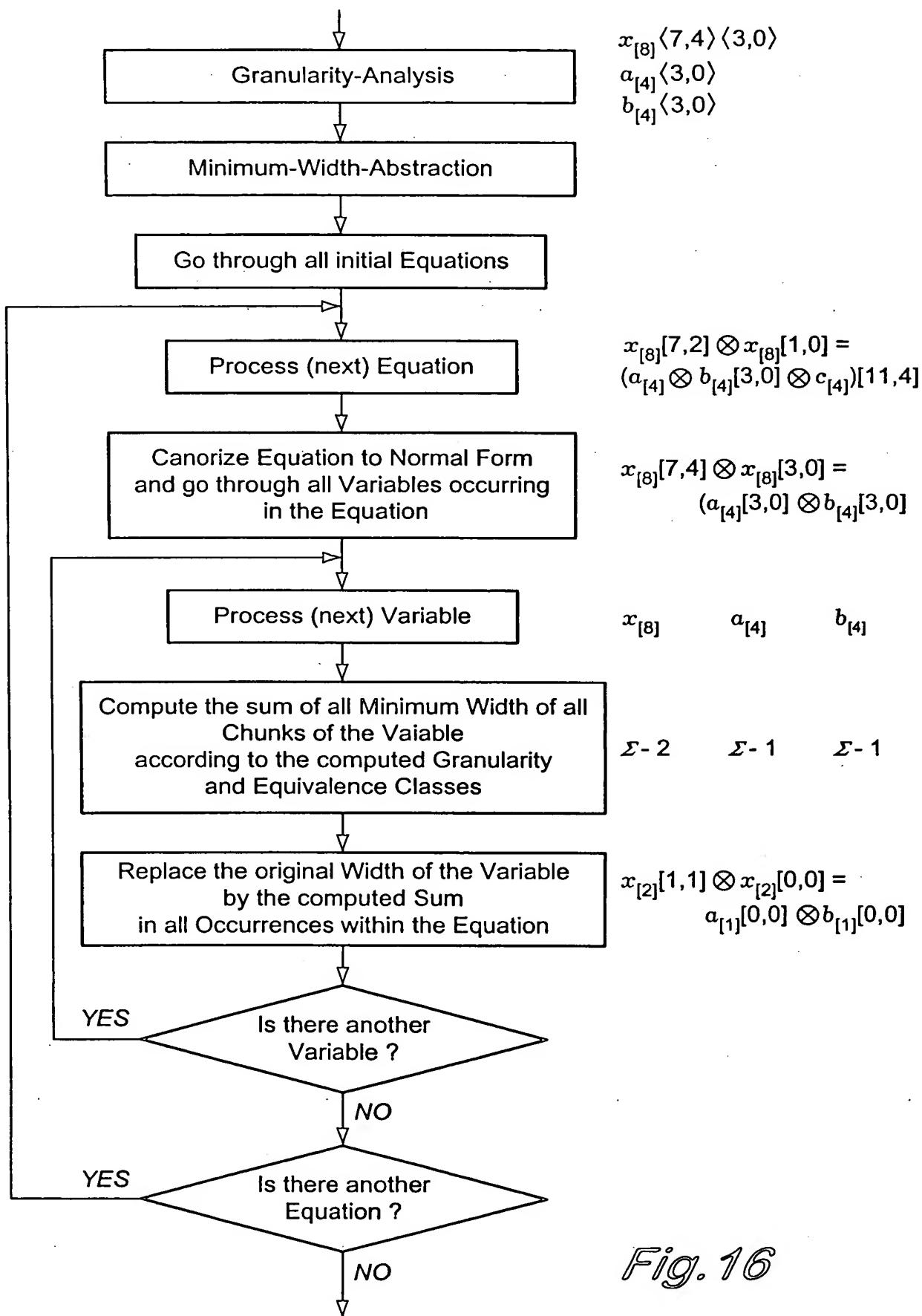
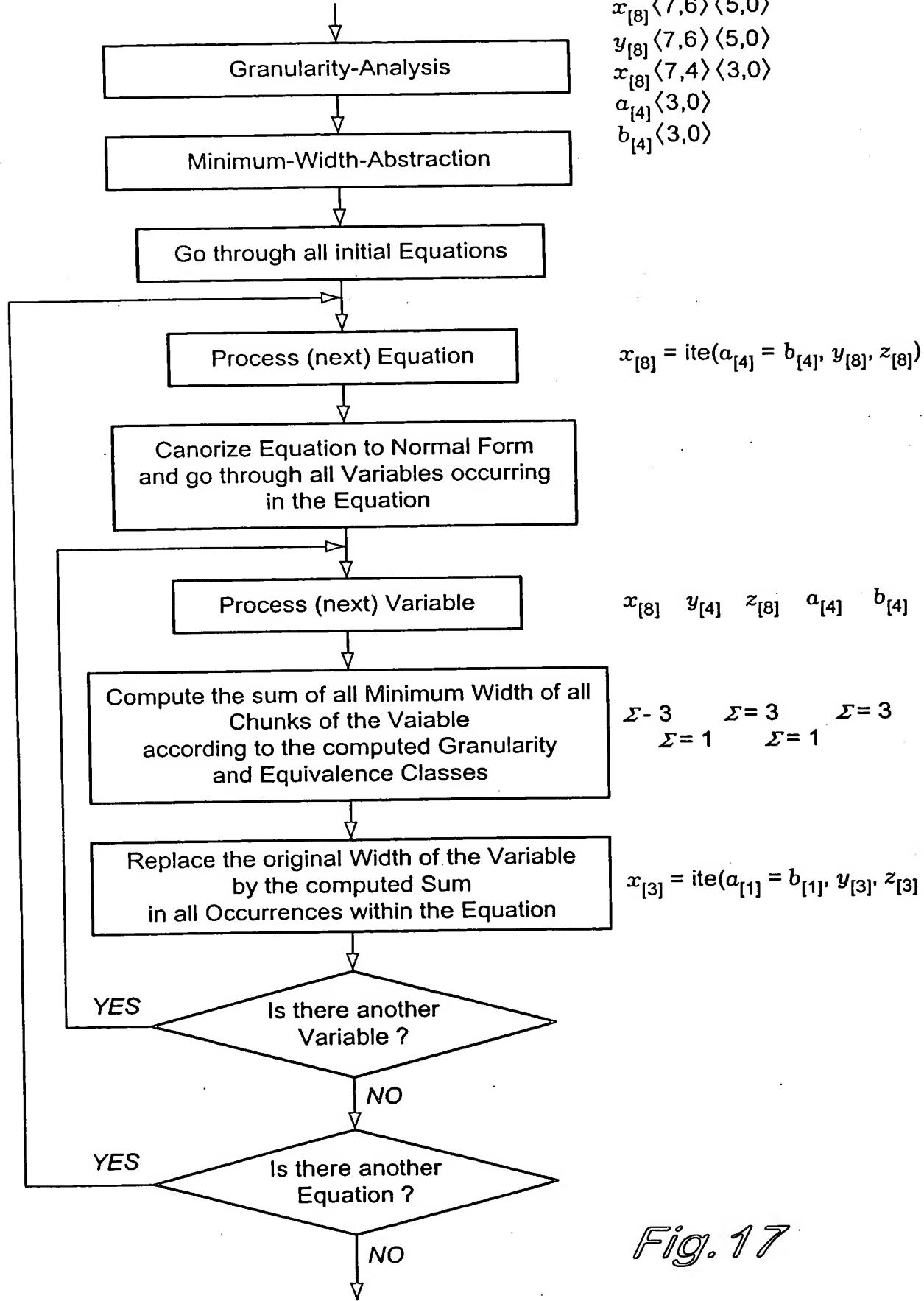


Fig. 16

18/19



40038870 040802

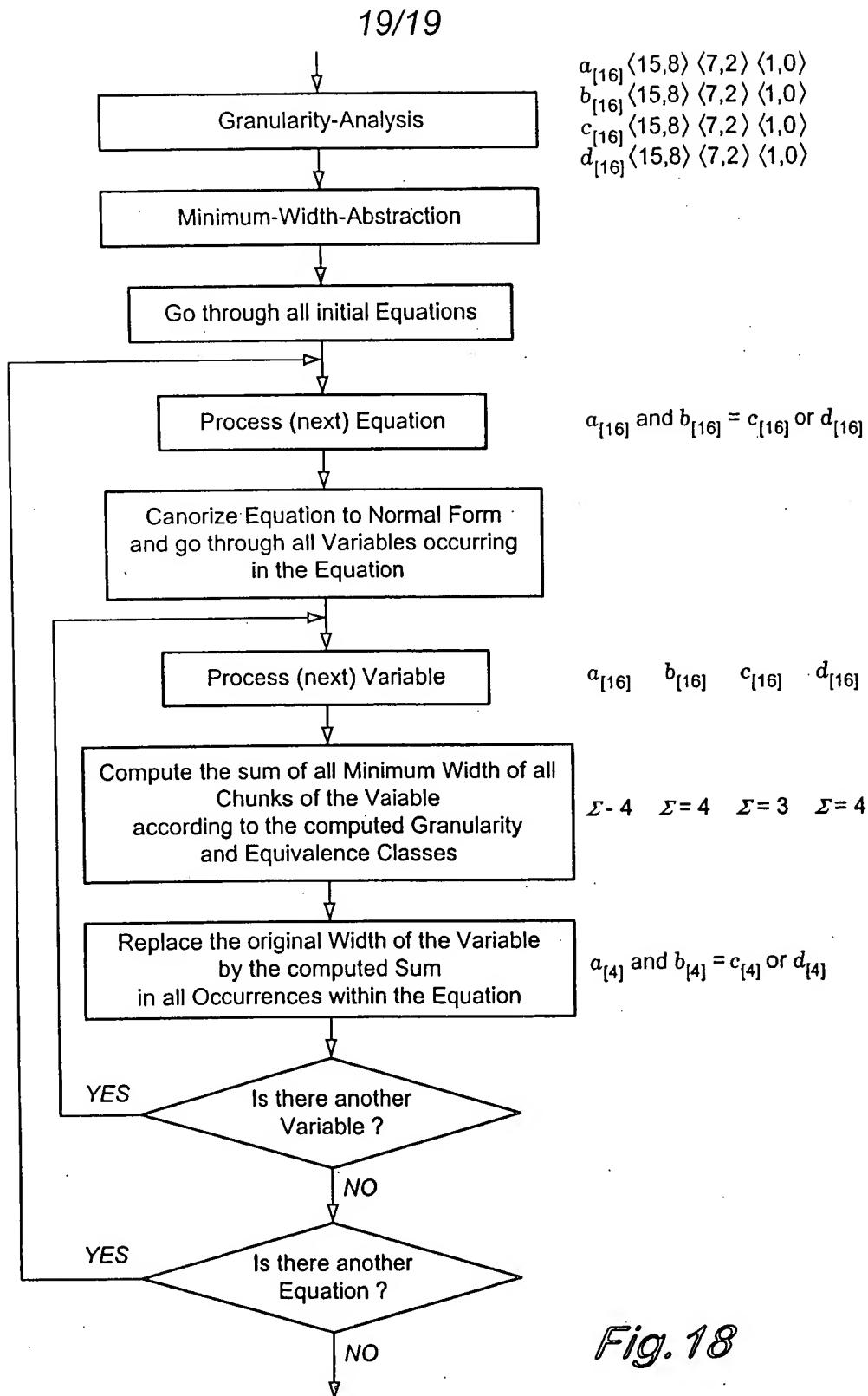


Fig. 18